УДК 681.3.07
И.В.Куржеевский, В.В.Бродовская, А.С.Папкова
Академия военно-морских сил имени П.С. Нахимова
Севастопольский национальный технический университет

АЛГОРИТМ СТОХАСТИЧЕСКОЙ АУТЕНТИФИКАЦИИ, ИСПОЛЬЗУЮЩИЙ ГАМИЛЬТОНОВЫ ЦИКЛЫ ГРАФОВ

Рассматривается алгоритм стохастической аутентификации, использующий для проверки подлинности пользователей знание ими гамильтонового цикла в графе. Осуществляется стохастическая перестановка столбцов матрицы смежности исходного графа, затем матрица расширяется путем введения случайных строк и столбцов и после последующего перемешивания элементов матрицы, шифруется по алгоритму RSA.

Ключевые слова: *стохастическая аутентификация, гамильтоновы циклы графов.*

Постановка проблемы. Развитие современных информационных технологий и широкое внедрение вычислительной техники во все сферы жизнедеятельности общества делает проблему защиты информации от несанкционированного доступа актуальной. При взаимодействии в сети субъектов (пользователей, процессов, действующих от имени определенных пользователей, или иных аппаратно-программных комплексов) возникает практически важная задача проверки подлинности этих субъектов. Аутентификация субъектов и сообщений [3] представляет собой процедуру, обеспечивающую связывающимся сторонам возможность проверки аутентичности (подлинности) взаимодействующих субъектов и получаемых сообщений. Широкое распространение получили протоколы двухсторонней строгой аутентификации, использующие различные криптографические средства, но, к сожалению, всегда возможна утечка информации об используемых секретных ключах. Поэтому необходимы дополнительные криптографические преобразования, позволяющие повысить криптостойкость (вычислительную стойкость) используемых протоколов аутентификацию. В качестве одного из вариантов повышения криптостойкости протоколов аутентификации авторы предлагают алгоритм стохастической аутентификации, использующий гамильтоновы циклы графов. Отличие предлагаемого алгоритма от существующих алгоритмов [1] состоит в том, что после случайной перестановки столбцов матрицы смежности исходного графа, матрица дополняется случайными строками и столбцами, но так, что остается квадратной, затем элементы матрицы стохастически перемешиваются и шифруются с помощью теории квадратичных вычетов и алгоритма RSA.

Цель статьи. Повышение за счет задания неопределенности хода шифрования информации вычислительной стойкости протокола двухсторонней строгой аутентификации пользователей, использующего знание ими гамильтонового цикла графа. Если в механизме шифрования будут использоваться операции или процедуры, зависящие от преобразуемых данных, тогда сами операции будут изменяться случайно. "Подмешивание" случайных данных к шифруемому аутентификационному сообщению позволит задать вероятностный характер операций преобразования информации, что затруднит использование общего принципа криптоанализа шифров, основанного на попытках выявления статистических свойств алгоритма шифрования, например, путем подбора специальных исходных текстов или криптограмм.

Изложение основного материала. Графом $G(V,E)$ называется совокупность двух множеств – непустого множества V (множества вершин) и множества E (множества ребер). Маршрутом в графе $G(V,E)$ называется чередующаяся последовательность вершин и ребер: $v_0, e_1, v_1, e_2, \ldots, e_k, v_k$, в которой любые два соседних элемента инцидентны. Если $v_0 = v_k$, то маршрут замкнут, иначе открыт. Если все ребра различны, то маршрут называется цепью. Если все вершины (а значит, и ребра) различны, то маршрут называется простой цепью. В цепи $v_0, e_1, v_1, e_2, \ldots, e_k, v_k$ вершины v_0 и v_k называются концами цепи. Замкнутая цепь называется циклом; замкнутая простая цепь называется простым циклом. Если граф имеет простой цикл, содержащий все вершины графа по одному разу, то такой цикл является гамильтоновым циклом, а граф называется гамильтоновым графом.

Предположим, что в графе G с n вершинами гамильтонов цикл существует, тогда при некоторой нумерации вершин он пройдет точно через вершины с последовательными номерами $1,2,\ldots,n$. Поэтому путем перебора всех возможных нумераций вершин, возможно, найти гамильтонов цикл. Но количество возможных нумераций равно $n!$ [1]. Доказано, что для нахождения гамильтонова цикла в графе, не существует определенного алгоритма, существенно более быстрого, чем указанный метод перебора. Задача нахождения гамильтонова цикла в графе, является *NP* полной [1, 2], поэтому возникает вопрос, а нельзя ли использовать данную задачу для решения вопроса аутентификации пользователей. Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности". Двумя важными задачами аутентификации является проверка того, что содержимое сообщения не было изменено, и того, что сообщение прибыло именно из того источника, о котором информирует сообщение [1-4]. Одной из распространенных схем аутентификации является простая аутентификация, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств их использования и обработки. Идея строгой аутентификации, реализуемая в криптографических протоколах, заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне [3], демонстрируя знание какого-либо секрета, который, например, может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена. Доказательство знания секрета осуществляется с помощью последовательности запросов и ответов с использованием криптографических методов и средств. В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов [3]:

1. Односторонняя аутентификация;

2. Двусторонняя аутентификация;

3. Трехсторонняя аутентификация.

Односторонняя аутентификация предусматривает обмен информацией только в одном направлении. Двусторонняя аутентификация по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с тем партнером, которому были предназначены аутентификационные данные. Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей. В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы [3, 4]:

1. Протоколы строгой аутентификации на основе симметричных алгоритмов шифрования;
2. Протоколы строгой аутентификации на основе ассиметричных алгоритмов шифрования;
3. Протоколы строгой аутентификации на основе алгоритмов электронной цифровой подписи (ЭЦП).

В данной работе предлагается алгоритм стохастической аутентификации, использующий гамильтоновы циклы графов. Отличие предлагаемого алгоритма от существующих алгоритмов [1] состоит в том, матрица смежности графа изоморфного исходному графу дополняется случайными строками и столбцами, но так, что матрица остается квадратной, затем элементы матрицы стохастически перемешиваются. Стохастическими методами принято называть методы защиты, прямо или косвенно основанные на использовании генераторов псевдослучайных последовательностей (ГПСП), при этом эффективность защиты в значительной степени определяется свойствами используемых генераторов псевдослучайных последовательностей.

Стохастический алгоритм строгой аутентификации, использующий гамильтоновы циклы графов, шифрование на основе теории квадратичных вычетов и ассиметричную систему защиты информации RSA, выполняется следующим образом:

1. Абонент А, участвующий в протоколе двухсторонней строгой стохастической аутентификации, зная исходный граф G, имеющий матрицу смежности размером $n \times n$, строит

изоморфный ему граф H . Для построения графа H в матрице смежности исходного графа осуществляется перестановка столбцов с помощью генератора псевдослучайных последовательностей (ГПСП) № 1 с ключом k_1.

2. С помощью ГПСП № 2 с ключом k_2 абонент А генерирует $m^2 - n^2$ случайных бит и формирует из них строки и столбцы расширенной (размером $m \times m$) матрицы смежности изоморфного графа H .

3. По результатам работы ГПСП № 3 с ключом k_3 абонент А осуществляет циклические сдвиги строк и столбцов на случайное для каждой строки и столбца число позиций и тем самым производит стохастическое перемешивание элементов полученной матрицы.

4. Элементы полученной матрицы шифруются с использованием квадратичных вычетов по заданному модулю следующим образом [2]. Если элемент в полученной матрице равен 0, то генерируется случайное число и возводится в квадрат по $mod\ n_2$, где n_2 - открытое число абонента В. Если число представляет собой квадрат некоторого числа по $mod\ n_2$, то это число является квадратичным вычетом по заданному модулю. Если элемент матрицы равен 1, то вычисляется квадрат любого числа и умножается на открытый ключ y, который является квадратичным невычетом, результат берется по $mod\ n_2$. В итоге полученное произведение так же будет квадратичным невычетом.

5. Затем полученная матрица шифруется открытым ключом абонента В по алгоритму RSA [4].

6. Зашифрованная матрица передается абоненту В.

7. Абонент В используя свой секретный ключ для алгоритма RSA расшифровывает полученную матрицу.

8. Дальнейшее расшифрование матрицы абонентом В основывается на математическом аппарате теории квадратичных вычетов. Для этого абонент В проверяет с помощью символа Якоби-Лежандра [2], являются ли элементы матрицы, квадратичными вычетами или невычетами. Если элемент матрицы квадратичный вычет, то он заменяется 0, если элемент матрицы квадратичный невычет, то его заменяют на 1.

9. Затем абонент В, используя ГПСП № 3 с ключом k_3, осуществляет циклические сдвиги строк и столбцов полученной матрицы, обратные циклическим сдвигам из пункта 3.

10. Добавленные в матрицу случайные строки и столбцы абонент В отбрасывает, так как знает размер матрицы смежности исходного графа.

11. Используя ГПСП № 1 с ключом k_1 абонент В осуществляет перестановку столбцов, обратную исходной перестановке и восстанавливает матрицу смежности графа. Затем определяет гамильтонов цикл в графе, соответствующем расшифрованной матрице смежности и убеждается в подлинности абонента А.

12. Для подтверждения своей подлинности, абонент В выполняет пункты 1-6 данного алгоритма, но для шифрования по методу RSA использует открытый ключ абонента А и производит вычисления в пункте 4 по $mod\ n_1$, где n_1 - открытое число абонента А. Затем зашифрованная матрица смежности пересылается абоненту А, который выполняет пункты 7-11 алгоритма и в случае положительного результата убеждается в подлинности абонента В. Таким образом происходит взаимная строгая стохастическая аутентификация абонентов.

Открытой информацией в предложенном алгоритме стохастической аутентификации являются:

1. открытые ключи абонентов А и В, необходимые для шифрования по алгоритму RSA расширенной и стохастически перемешанной матрицы смежности исходного графа;

2. модули n_1 и n_2, которые используют, соответственно, абоненты А и В для шифрования и расшифрования по алгоритму RSA, а также для генерации квадратичных вычетов и невычетов;

3. открытый ключ y данного алгоритма стохастической аутентификации, необходимый для вычисления квадратичных невычетов по заданному модулю.

Секретной информацией в данном алгоритме являются:

1. секретные ключи абонентов А и В;

2. матрица смежности исходного графа, гамильтонов цикл в этом графе и количество вершин в этом графе;

3. секретные ключи k_1, k_2 и k_3, необходимые для работы генераторов псевдослучайных последовательностей, используемых для перестановки строк, генерации случайных бит и циклических сдвигов каждой строки и столбца расширенной матрицы смежности на случайное для каждой строки и столбца число позиций.

Для атаки на предложенный алгоритм стохастической аутентификации злоумышленнику необходимо:

1. по открытым ключам абонентов А и В попытаться вычислить их секретные ключи, что при достаточной длине чисел n_1 и n_2 является на данный момент вычислительно неразрешимой задачей за приемлемое машинное время;

2. определить, какие элементы в расшифрованной, расширенной и перемешанной матрице смежности являются квадратичными вычетами, а какие невычетами, что без решения задачи разложения чисел n_1 и n_2 на простые множители (решения задачи факторизации) также вычислительно невозможно за приемлемое машинное время;

3. вычислить секретный ключ k_3 и осуществить обратную циклическую перестановку элементов расшифрованной матрицы смежности;

4. попытаться определить размер матрицы исходного графа для того, чтобы отбросить случайные строки и столбцы в расшифрованной матрице смежности;

5. взломать генератор псевдослучайных последовательностей № 1 и найти ключ k_1, а затем осуществить обратную перестановку столбцов матрицы смежности и определить гамильтонов цикл в полученном графе.

Оценим вычислительную стойкость предложенного алгоритма стохастической аутентификации пользователей, использующего знание ими гамильтонового цикла в графе, с точки зрения взлома методом полного перебора. Пусть матрица смежности исходного графа имеет размер $n \times n$, тогда путем перестановки ее столбцов можно получить $n!$ матриц смежности графов изоморфных исходному. Размер матрицы с переставленными столбцами увеличивается до $m \times m$. Для этого генерируются $m^2 - n^2$ случайных значений 0 и 1, из которых формируются случайные строки и столбцы. Так как далее элементы матрицы стохастически перемешиваются за счет циклических сдвигов строк и столбцов, то количество возможных вариантов выборки элементов матрицы размером $n \times n$ из элементов матрицы $m \times m$ можно вычислить по формуле для числа размещений $A_{m^2}^{n^2} = \frac{[(m]^2)!}{[(m]^2)! - [(n]^2)!}$. Злоумышленник не знает разложения чисел n_1 и n_2 на простые множители, поэтому вероятность того, что он правильно определит, является ли

данное элемент матрицы квадратичным вычетом или невычетом равна . Так как число элементов в матрице равно m^2, то вероятность правильного определения всех элементов матрицы составит . Таким образом, общее количество возможных вариантов вычисляется по формуле $N = n! \cdot A_{m^2}^{n^2} \cdot 2^{m^2}$.

Выводы. За счет случайной перестановки столбцов матрицы смежности исходного графа с гамильтоновым циклом, расширения этой матрицы смежности путем "подмешивания" случайных данных и последующего шифрования с использованием квадратичных вычетов и алгоритма RSA предложенный алгоритм стохастической аутентификации пользователей обладает высокой вычислительной стойкостью. Например, если матрица смежности исходного графа имеет размер 10×10, а расширенная матрица 20×20, то количество возможных вариантов, необходимых для полного взлома данного протокола аутентификации составит приблизительно $N \approx 10^{382}$. Предложенный алгоритм был реализован на языке Pascal в среде Aribasw. Результаты тестирования алгоритма на правильность результатов шифрования и расшифрования показали его работоспособность. Созданный алгоритм может быть использован в качестве составной части программных комплексов защиты информации от несанкционированного доступа.

1. Рябко Б.Я. Криптографические методы защиты информации / Б.Я.Рябко, А.Н. Фионов М.: Горячая линия-Телеком, 2005. - 229 с.
2. Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко, Санкт-Петербург: АНО НПО "Профессионал", 2004. – 478 с.
4. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер - М.: Издательство ТРИУМФ, 2003. – 816 с.